UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Three phones, currently located at the U.S. Department of Homeland Security evidence locker located at 790 North Milwaukee Street, #600, Milwaukee, Wisconsin, further described on Attachment A.	)	Case No. 25-814M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 2/25/2025 *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nancy Joseph.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 2/11/2025 @ 11:49 a.m.

Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

The property to be searched are as follows:

a. black Vortex, Model A24 cellular telephone, barcode: 3020240921170144412923, IMEI #: 358645341772515.

b. black Samsung Galaxy A15, Model SM-A156U cellular telephone, IMEI #: 358103210458931.

c. black Samsung Galaxy A13, Model SM-A135U cellular telephone, IMEI #: 357630390330382.

The Devices are currently located at the U.S. Department of Homeland Security-Homeland Security Investigations evidence locker located at 790 North Milwaukee Street, #600, Milwaukee, Wisconsin 53202.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of 18 USC 2252 and 2252A, including:

   a. Records containing child pornography or pertaining to the production, distribution, receipt, or possession of child pornography;

   b. Records or information, photographs, videos, notes, documents, or correspondence, in any format or medium, concerning communications about child pornography or sexual activity with or sexual interest in minors.

2. All names, aliases, and numbers stored in the Devices, including numbers associated with the Devices, relating to the identities of those engaged in the production, possession, receipt, or distribution of child pornography.

3. Images or visual depictions of child pornography.

4. Records and information containing child erotica, including texts, images, and visual depictions of child erotica.

5. Any and all information, notes, software, documents, records, or correspondence, in any format and medium, pertaining to the violations.

6. Any and all address books, names, and lists of names and addresses of individuals who may have been contacted by use of the computer or by other means for the purpose of committing the violations.

7. The list of all telephone calls made or received located in the memory of the Devices that provides information regarding the identities of and the methods and means of operation and communication by those engaged in the possession, receipt, or distribution of child pornography.

8. Any and all information, notes, documents, records, or correspondence, in any format or medium, concerning membership in online groups, clubs, or services that provide or make accessible child pornography.

9. Any and all information, records, documents, invoices, and materials, in any format or medium, that concern e-mail accounts, online storage, or other remote computer storage pertaining to the violations.

10. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Three phones, currently located at the U.S. Department of Homeland Security evidence locker located at 790 North Milwaukee Street, #600, Milwaukee, Wisconsin, further described on Attachment A.	Case No. 25 814M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Please see Attachment A.

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(5)(B) 18 U.S.C. §§ 2252A(a)(2)(A and (b)(1)	Possession of and access with intent to view child pornography and receipt of child pornography

The application is based on these facts:

Please see Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Tyler J. L'Allier, Task Force Officer - HSI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 2/11/2025

Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph - Magistrate Court Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Tyler J. L'Allier, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property— electronic device—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Task Force Officer (TFO) with the Department of Homeland Security, Homeland Security Investigations (HSI), an investigative branch of the United States Department of Homeland Security. I am a federal law enforcement officer authorized by the Secretary of Homeland Security to request the issuance of criminal complaints and search warrants. As a TFO, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I have been employed as a TFO with HSI since August 2024. I am currently assigned to the Resident Agent in Charge Office in Milwaukee, Wisconsin.

3. My experience as a HSI TFO have included the investigation of cases involving the use of computers and the Internet to commit violations of federal law involving child exploitation, including the production, transportation, receipt,

distribution, and possession of child pornography. I am also a Detective with the Washington County Sheriff's Office assigned to the Major Crimes Unit and have been employed in this capacity since July 29, 2021; prior to that I was an Investigator assigned to the Major Crimes and before that I was an Investigator assigned to the Multijurisdictional Drug Enforcement Group. I have eighteen years of Law Enforcement experience. I have experience working complex criminal investigations including, violent crimes, narcotics, financial crimes, sexual assaults, and child abuse/child sexual assaults. I have attended many different trainings on the investigations of many law enforcement criminal investigative topics, including the United States Department of Justice 2023 National Law Enforcement Training on Child Exploitation, ICAC Investigative Techniques, Department of Justice - Division of Criminal Investigations 'Drug Investigator School', controlled substance trafficking, death investigations, identity theft/ financial crimes, interview and interrogation techniques, internet crimes, and child exploitation investigations. I have worked many sexual assault and sexual assault of children cases as well as child maltreatment related cases. I have worked jointly with state, and local investigators in cases of sexual assault, possession and/or distribution of child pornography. I have received training and have gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications and the execution of searches and seizures involving computer crimes. I have investigated and assisted in the investigation of criminal

matters involving the sexual exploitation of children which constituted violations of Title 18, United States Code, Sections 2251, 2252 and 2252A.

4. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A, incorporated herein by reference as if fully set forth, are located on the Devices for which authority is requested to search. Where statements of others are set forth in this affidavit, they are set forth in substance and in part.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. The property to be searched are as follows ("Devices"):

a. black Vortex, Model A24 cellular telephone, barcode: 3020240921170144412923, IMEI #: 358645341772515.

b. black Samsung Galaxy A15, Model SM-A156U cellular telephone, IMEI #: 358103210458931.

c. black Samsung Galaxy A13, Model SM-A135U cellular telephone, IMEI #: 357630390330382.

6. The Devices are currently located at the U.S. Department of Homeland Security-Homeland Security Investigations evidence locker located at 790 North Milwaukee Street, #600, Milwaukee, Wisconsin 53202. In my training and experience, I know that the Devices have been stored in a manner in which its contents are, to the

extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of HSI.

7. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

8. The purpose of this application is to seize evidence of violations of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography) and 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (receipt of child pornography).

BACKGROUND ON NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN

9. Based on my training and experience, and publicly available information, I know that the National Center for Missing and Exploited Children (NCMEC) is a nonprofit organization in Alexandria, Virginia, that works with law enforcement on issues related to missing and sexually exploited children. One of the services provided and administered by NCMEC is its CyberTipline, which serves as the national clearinghouse for leads regarding sexual exploitation crimes against children.

10. In addition to reports from the general public, reports are made by U.S. electronic communication service (ECS) providers and remote computing services (RCS), which are required by 18 U.S.C. § 2258A to report "apparent child pornography" to NCMEC via the CyberTipline if they become aware of the content on their servers. Specially trained analysts, who examine and evaluate the reported content, review leads, add related information that may be useful to law enforcement, use publicly

available search tools to determine the geographic location of the apparent criminal act, and ultimately provide all of the gathered information to the appropriate law enforcement agency for review and possible investigation.

11. The CyberTipline receives reports, known as CyberTips, about the possession, production, and distribution of child pornography; online enticement of children for sexual acts; child prostitution; sex tourism involving children; child sexual molestation; unsolicited obscene material sent to a child; misleading domain names; and misleading words or digital images on the Internet.

12. The CyberTip reports will vary in detail depending on the nature of the report, and which entity submits it. The reports can include information (1) relating to the identity of any individual who appears to have violated federal law by committing or attempting to commit the criminal conduct described above; (2) historical information on when or how a customer or subscriber of an ECS or RCS uploaded, transmitted, or received apparent child pornography; (3) geographical information on the involved individual or website, which may include the IP Address or verified billing address or geographic identifying information, including area code or zip code; (4) any images of apparent child pornography; and (5) the complete communication containing any image of apparent child pornography.

BACKGROUND INFORMATION REGARDING SNAPCHAT

13. Snapchat is one of the most popular applications for sending and receiving 'self-destructing' messages, pictures, and videos. Referred to as 'snaps', the

company processes approximately 700 million of them every day on Apple's iOS and Google's Android operating systems. Snapchat users access the application frequently. According to marketing material provided by the company the average Snapchat user checks their account 14 times a day.

14. Snapchat is headquartered in Santa Monica, California, and owns and operates a free access social networking website of the same name that can be accessed at http://www.snapchat.com. Snapchat is one of the most popular applications for sending and receiving 'self-destructing' messages, pictures, and videos.

15. A "snap" is a picture or video message taken and shared with other Snapchat users in real-time. The sender of a snap has the option of setting a timer for how long a snap can be viewed. Once a snap has been viewed it is deleted from the company's system and is no longer visible to the recipient. Snapchat users can send text messages to others using the Chat feature. Once a user leaved the Chat screen, messages viewed by both the sender and the receiver will no longer be visible. The application notifies other users when they are online so they can begin messaging each other. In addition, Snapchat users can send pictures to other users by utilizing the camera on their device. Pictures can also be sent from the saved pictures in the photo gallery of the device. Accessing a Snapchat account and "snaps" constitute "electronic communications" within the meaning of 18 U.S.C. § 3123. *See* 18 U.S.C. §§ 3127(1) and 2510(12).

16. "Our Stories" is a collection of user submitted "Snaps" from different locations and events. A Snapchat user, with the location services of their device turned on, can contribute to a collection of snaps regarding the event. For example, multiple different Snapchat users at a rave could all contribute to the same "Our Stories" collection by sharing their snaps, even if they do not know each other. Users can also view "Our Stories" events if they are not actually present at the event by subscribing to the story. In addition to "Our Stories", a Snapchat user can keep a sort of photo/video diary using the "Story" feature. Each snap in a "Story" documents the user's experience. Based on the user's privacy settings, the photos and videos added to a "Story" can be viewed either by everyone on Snapchat or just the user's friend. Stories are visible to other users for up to 24 hours.

17. While a Snapchat message may disappear, the record of who sent it and when still exists. Snapchat records and retains information that is roughly analogous to the call detail records maintained by telecommunications companies. This includes the date, time, sender, and recipient of a snap. Additionally, Snapchat stores the number of messages exchanged, which users they communicate with the most, message status including if and when the message was opened, and whether the receiver used the native screen capture function of their device to take a picture of the snap before it disappeared.

18. Snapchat asks users to provide basic contact and personal identifying information to include date of birth. When a user creates an account, they make a unique Snapchat username. This is the name visible to other Snapchat users. An email address is required to register a Snapchat account, and a new user must also provide a

mobile phone number. This phone number is verified during the registration process. Snapchat sends an activation code, which must be entered before proceeding with the registration step. However, a user may elect to bypass entering a phone number so one may not always be present in the user's account. Snapchat also retains the account creation date.

19. Snapchat stores device information such as the model, operating system, operating system version, mobile device phone number, and mobile network information of devices used in conjunction with the service. They also collect unique device identifiers such as the Media Access Control (MAC) address and the International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of devices used to access Snapchat. In the event the Snapchat user's application crashes, the company also collects a list of other installed applications on the device to detect any potential software conflicts.

BACKGROUND INFORMATION REGARDING KIK MESSENGER

20. Kik Messenger (Kik), owned by MediaLab.AI. Inc. is designed for mobile chatting or messaging. To use this application, a user downloads the application to a mobile phone or other mobile device via a service such as Google Play Store, Apple iTunes, or another similar provider. Once downloaded and installed, the user is prompted to create an account and username. The user also has a display name, which is what other users see when transmitting messages back and forth.

21. As part of the account creation process, Kik users are asked to supply an e-mail address, create a password, provide an optional date of birth, and user location. The user also has the option of uploading a "profile avatar" that is seen by others. Once the Kik user has created an account, the user is able to locate other users via a search feature, and allows the parties to send each other messages, images, and videos. The search feature usually requires the user to know the intended recipient's username. Once another user is located or identified, Kik users can send messages, images, and videos between two parties.

22. Kik also allows users to create chat rooms of up to 50 people to communicate in a group setting and exchange images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. These groups are frequently created with a "hashtag" that is easily identifiable or searchable by keyword.

23. Kik Messenger users frequently advertise their Kik usernames on various social networking sites to meet and connect with other users. In some cases, Kik also provides various avenues, such as dating sites and social media applications, for meeting other users. HSI undercover agents have noted messages posted in Kik Messenger chat rooms relating to the enforcement, deletion, or banning of users and rooms by Kik messenger for the purpose of exchanging or distributing child pornography. HSI agents noted the comments to include the continued creation of new rooms and new user accounts to circumvent Kik Messengers enforcement efforts.

PROBABLE CAUSE

Information Obtained from the Kenosha Police Department

24. On November 18, 2024, I was provided investigative lead information from Kenosha Police Department (KPD) Detective Ashley Dobbe and Officer Megan Hird regarding Randy C. SMITH (DOB 05/21/1979), a registered sex offender believed to be previously residing in Kenosha, Wisconsin. Initial lead information indicates SMITH is the subject of three CyberTips received from NCMEC. Attempts to locate SMITH by the KPD were unsuccessful.

25. According to KPD case #2024-00012920, on March 22, 2024, KPD Detective Peter Deates received NCMEC CyberTip #179292096. According to NCMEC CyberTip #17292096, on November 12, 2023, at approximately 08:27:52 CST and November 13, 2023, at approximately 12:38:31 CST, Snapchat username "randys9535" saved, uploaded, or shared two files of apparent child sexual abuse material (CSAM). The following subscriber information was provided by Snapchat for "randys9535":

> Phone: +2623440877 (verified)[1]
> Date of Birth: May 21, 1979
> Email Address: randycsmith0@gmail.com (verified)
> Internet Protocol (IP) address: 75.184.100.224 (Login), November 12, 2023, 08:32:28 CST

[1] An email address is required to register a Snapchat account, and a new user must also provide a mobile phone number. This phone number is verified during the registration process. Snapchat sends an activation code, which must be entered before proceeding with the registration step.

26. On March 7, 2024, an administrative subpoena was issued by the State of Wisconsin – Office of the Attorney General requesting subscriber records associated with IP address 75.184.100.224 being utilized on November 12, 2023, at 08:32:28 CST.

27. On March 20, 2024, Charter Communications produced the following subscriber records for the aforementioned IP address:

> Subscriber Name: Toni Smith[2]
> Service Address: 5401 38th Ave., Kenosha, WI 53144-2719
> Account Number: 8348100580328955
> Lease Log: Start Date: May 19, 2022
> End Date: March 15, 2024

28. On March 25, 2024, the Kenosha County Circuit Court authorized a warrant for communication/records from October 13, 2023, through November 30, 2023, associated with Snapchat username "randys9535".

29. On April 11, 2024, Snapchat produced the requested records pursuant to the issued search warrant. Records received indicate the account associated with Snapchat username "randys9535" was created on November 5, 2023, utilizing IP address 75.184.100.224. A verified email address of randycsmith0@gmail.com and telephone number of (262) 344-0877 were provided by the user. A date of birth of May 21, 1979, was also noted. In addition to subscriber records, Snapchat also produced Artificial Intelligence (AI) conversations, call logs, chat conversations to include associated media files, IP records, and friends.

---

[2] Based on database queries, Toni Smith is believed to be the mother of Randy C. SMITH.

30. On January 10, 2025, I reviewed AI conversations associated with this account. Records indicate on November 6, 2023, and November 13, 2023, this user asked the AI platform, "Find teen girls", "All teen girls to chat with", "Find some girls ages 12 to 15 on snap", and "Find 13yo girls."

31. According to chat conversations I reviewed, on November 12, 2023, at 08:27:52 p.m. CST, Snapchat user "randys9535" uploaded a file labeled as de850391-9067-56ce-bd41-846267063026-15. I reviewed this file which is described as follows:

> *This file is described as a still, color image which depicts a prepubescent female sitting back on a tan colored chair with her knees pulled up to her chest. The prepubescent female has red hair in ponytails held up with puffy white hair ties. She has a light-colored shirt and multi-colored underwear pulled just below her knees. Her legs are spread apart exposing her vagina and anus, which appear to be the focal point of the photograph. The prepubescent female does not have any pubic hair.*

Based on my training and experience, the image as described above depicts child pornography.

32. On November 13, 2023, at 12:38 a.m. CST, Snapchat user "randys9535" uploaded a filed labeled as 5de5ca3c-8c1f-5a63-8e62-7e945aabe63c-36. I reviewed this file which is described as follows:

> *This file is described as a still, color image which depicts a prepubescent white female either standing or kneeling between the legs of an adult white male who*

has an erect penis. The adult male is not wearing any clothing and looks to be sitting. The prepubescent female is holding onto the top of the erect penis with her right hand and is looking at the camera smiling. She appears to have dental braces on her teeth. The female is wearing a blue t-shirt with a yellow design on the front of it and is wearing a green "trucker" hat.

Based on my training and experience, the image as described above depicts child pornography.

33. A review of additional files indicates on November 13, 2023, at 12:45:11 a.m. CST, Snapchat user "randys9535" distributed a file labeled as b~ChdoekdHdXNyaFp0bUlPNWVYanM0M2hfMRIlEhVoekdHdXNyaFp0bUlPNWVY anM0M2gaABoAMANIAVAEYAFwAg to "baddie_girl". I reviewed this file which is described as follows:

This file is described as a still, color image which depicts a white adult male with an erect penis ejaculating into the mouth of what appears to be a prepubescent female. Sperm (Ejaculate) can be seen on the female's tongue.

Based on my training and experience, the image as described above depicts child pornography.

34. On November 28, 2023, Snapchat user "randys9535" shared three images with user "tsthroatbaby23." After reviewing a Wisconsin driver's license photo for Randy C. SMITH, the images sent appear to depict Randy C. SMITH.

35. A review of IP data received indicates on November 13, 2023, all account activity was associated with IP address 75.184.100.224, which as previously noted was assigned to Charter Communications subscriber Toni Smith, 5401 38th Ave., Kenosha, Wisconsin.

36. According to KPD case #2024-24343, on May 23, 2024, KPD Detective Peter Deates received CyberTip #183458486 from NCMEC. According to NCMEC CyberTip #183458486, on January 2, 2024, at 1:17:07 a.m. CST, Snapchat username "randys9535" saved, uploaded, or shared a file labeled as randys9535-None-f4e12068-1130-5376-9079-801d42c1db83~57-6677cf0c95-content.jpg which allegedly depicts CSAM based on a hash value match. The following subscriber information was provided by Snap Chat for "randys9535":

> Phone: +2623440877 (verified)
> Date of Birth: May 21, 1979
> Email Address: randycsmith0@gmail.com (verified)
> Internet Protocol (IP) address: 172.58.15.171 (Login), January 2, 2024, 01:45:59 a.m. CST

37. The KPD determined the Snapchat username associated with this CyberTip was the same username listed in CyberTip 179292096. No additional investigative activity occurred.

38. According to KPD case #2024-53313, on October 11, 2024, KPD Detective Ashley Dobbe received NCMEC CyberTip #197907977. According to CyberTip #197907977, on August 2, 2024, at 5:28:21 p.m. CST to August 2, 2024, at 6:16:58 p.m. CST, Kik Messenger user "jsmmoo" (screen name "Jsmmoo", ESP user ID:

"jsmmoo_kic) distributed twenty-six files which depicted CSAM to another user via a private message. These files were reviewed by Kik Messenger personnel based on a hash value match and determined to depict apparent CSAM. The listed, unconfirmed email address associated with this account is Randycsmith0@gail.co. Account login records provided indicate from August 2, 2024, at 11:19:51 a.m. CST, to August 2, 2024, at 6:24:48 p.m. CST, this account was accessed from IP address 72.131.94.44. Subscriber records provided indicate on August 2, 2024, at 1:19:51 p.m. CST, this account was registered from a Samsung device with Android identification number 9627a4e1402fa355.

39. Information provided by Kik Messenger indicates on August 2, 2024, at 6:07:41 a.m. CST, a CSAM file labeled as f21ae5aa-5edc-4b57-92ea-3e66772289be.jpg was uploaded by user "jsmmoo" and sent to another user via a private chat message utilizing IP address 72.131.94.44.

40. On October 7, 2024, State of Wisconsin – Office of the Attorney General issued an administrative subpoena to Charter Communications requesting subscriber records for IP address 72.131.94.44 being used on the date and time.

41. On October 11, 2024, Charter Communications produced the following subscriber records:

Subscriber Name: Toni Smith
Service Address: 5401 38th Ave., Kenosha, WI 53144-2719
Account Number: 8348100580328955
Lease Log: Start Date: May 25, 2024
End Date: October 9, 2024

42. On October 17, 2024, a warrant was authorized by the Kenosha County Circuit Court and issued to Kik, c/o MediaLab.ai. Inc. for communication/records associated with Kik Messenger user "jsmmoo" from July 1, 2024, to September 30, 2024.

43. On November 12, 2024, Kik, c/o MediaLab.ai. Inc. produced the requested records. Records received indicate on August 2, 2024, at 12:07:42 a.m. CST, "jsmmoo" sent numerous files utilizing IP address 72.131.94.44 which depict CSAM. One file sent to Kik user ID "maniblack7767_ox1" and labeled as f21ae5aa-5edc-4b57-92ea-3e66772289be.jpg is described as follows:

> *This file is described as a still, color image which depicts a prepubescent female lying on a bed fully unclothed looking at whomever is taking the photograph from behind her. An adult white male has his erect penis inserted into the vagina of the prepubescent female. The adult male has his left hand on the right buttock and thigh of the prepubescent female.*

44. A review of additional files sent by Kik user "jsmmoo" indicates on August 2, 2024, at 5:46:28 p.m. CST, a file labeled as e413cf0f-3ced-4fcb-8f5d-3e7d1e61200e.jpg was sent to Kik user ID "maniblack7767_ox1" and is described as follows:

> *This file is described as a still, color image which depicts a naked prepubescent female who is lying down with her legs pulled back towards her body. Her legs are apart exposing her vagina and anus. There is writing on the prepubescent*

females' chest that reads, "FUCK ME" with an arrow pointing directly at her vagina. The prepubescent female has no breast development or pubic hair.

Based on my training and experience, the image as described above depicts child pornography.

45. On August 2, 2024, at 6:16:55 p.m. CST, a file labeled as 350c5049-bf10-487b-b388-9e007c1637c5.jpg was sent to Kik user ID "copirw_unm" and is described as follows:

This file is described as a still, color image which depicts a prepubescent female who is naked lying on a pink blanket covered in white stars. Her legs are spread apart, and she is using her arms to hold them back to expose her vagina and anus to the camera. The prepubescent female has a pink object inserted into her vagina. She appears to be using her hands to expose more of her vagina. The prepubescent female has no breast development or pubic hair.

Based on my training and experience, the image as described above depicts child pornography.

46. A review of content provided indicates from August 3-4, 2024, there consisted of twenty-nine files which depict CSAM distributed by Kik user "jsmmoo" to other users while using the chat platform. Images and videos of an adult penis where also distributed on several instances.

47. On October 16, 2024, KPD Officer Megan Hird utilized law enforcement databases to determine on September 21, 2024, SMITH sold a cellular telephone via ecoATM at a kiosk located at a Walmart in Mount Pleasant, Wisconsin. After contacting ecoATM law enforcement support, Officer Hird learned the cellular telephone, a Vortex, model A24, was not data wiped. Also provided to Officer Hird were several images of SMITH selling the device at the kiosk, as well as his tendered Wisconsin driver's license.

48. On November 18, 2024, the device was turned over HSI and has remained in the HSI evidence locker.

49. On December 17, 2024, a subpoena was issued to Google LLC requesting records to be produced for email account randycsmith0@gmail.com, the verified email address associated with the previously noted Snapchat and Kik accounts.

50. On December 18, 2024, Google provided records indicating this account was created on October 24, 2023. The name listed for this account is "Randy Smi." IP login records were provided from March 24, 2024, to December 17, 2024. Records received indicate on several occasions from May 28, 2024, to August 8, 2024, this account was accessed from IP address 72.131.94.44 and 2603:6000:d401:3814:89fd:c98e:dec3:137a.

51. A Google Pay customer profile for this account lists the following information:

Account Holder Name: Randy C. Smith
Card Scheme: Mastercard
Account Number: ****8281 (created December 23, 2023)

52. On December 26, 2024, a subpoena was issued to Charter Communications requesting subscriber records associated with IP addresses 72.131.94.44 and 2603:6000:d401:3814:89fd:c98e:dec3:137a being utilized on various dates.

53. On January 2, 2025, Charter Communications provided the following subscriber records for these IP addresses:

Subscriber Name: Toni Smith
Service Address: 5401 38th Ave., Kenosha, WI 53144-2719
Account Number: 8348100580328955

54. On January 10, 2025, a subpoena was issued to T-Mobile requesting subscriber records for telephone number (262) 344-0877, the verified telephone number listed for the previously noted Snapchat and Kik accounts.

55. On January 18, 2025, T-Mobile produced the following subscriber records for telephone number (262) 344-0877:

Subscriber Name: Randy Smith
Address: 5401 38th Ave., Kenosha
Subscriber Status: Active
Subscriber Name Effective Date: November 5, 2023

56. On January 24, 2025, at approximately 2:13 p.m., the Racine County Sheriff's Office received a telephone call regarding a suicidal subject in the area of

Interstate 94 and Seven Mile Road. Deputies later identified this subject as Randy SMITH. SMITH indicated he was angry because his vehicle was towed. SMITH was placed into custody and transported to Aurora Hospital for evaluation. Two cellular telephones, later determined to be a black Samsung Galaxy A15, Model SM-A156U and black Samsung Galaxy A13, Model SM-A135U, were seized from SMITH and turned over to the Kenosha Police Department due to their ongoing investigation.

57. On January 28, 2025, the cellular telephones were turned over to HSI and have remained in the HSI evidence locker.

PRIOR CONVICTION FOR POSSESSION OF CHILD PORNOGRAPHY

58. I have reviewed a Criminal Complaint (Case No. 17-M-079) issued by the U.S. District Court for the Eastern District of Wisconsin on June 15, 2017. According to the affidavit in support of the criminal complaint, between March 1, 2017, and March 4, 2017, a special agent with the Federal Bureau of Investigation (FBI) observed ChatStep.com[3] user "hornydad" in a chatroom entitled "Pedo2," post three Dropbox links[4] which contained numerous files which depicted CSAM and child erotica. IP

[3] ChatStep.com is a web-based chatroom application which allows users to create anonymous usernames to chat and share files with other users.

[4] Dropbox is a privately held electronic file storage service provider which utilizes cloud computing to enable users to store and share files and folders with other users across the Internet by way of file synchronization. Once a file is added to a user's Dropbox account, that file is synced to Dropbox's secure online servers. Dropbox provides both free and fee based electronic file storage services.

login records associated with this account resolved to Time Warner Cable customer Randy SMITH, 4415 12th Street, Kenosha, Wisconsin.

59. On June 15, 2017, special agents with the FBI executed a search warrant at the residence of Randy SMITH. During a consensual interview conducted with SMITH, he acknowledged he had distributed CSAM files utilizing Dropbox, Chatstep, and Kik. He advised he had used Kik to trade CSAM files via Dropbox with approximately thirty Kik contacts who were also interested in CSAM.

60. On this date, SMITH allowed law enforcement to search his Dropbox account. This account contained approximately 1,016 files. A majority of these file depicted CSAM.

61. On September 8, 2017, Randy SMITH appeared in U.S. District Court for the Eastern District of Wisconsin for a sentencing hearing. On this date, SMITH was sentenced to three years in prison followed by five years of supervised release for two counts of Possession of Child Pornography. SMITH was released from prison on May 6, 2021.

62. On February 24, 2022, SMITH's supervised release was revoked for the following violations: failure to refrain from unlawful use of controlled substances, failure to submit urine tests, unknown whereabout and activities of the defendant, failure to report place of employment, failure to not commit another federal, state, or local crime, possessing two SIM cards and an Alcatel smartphone, and attempting to

obtain child pornography. SMITH was sentenced to four months in prison. He was released from prison on March 24, 2022.

63. On May 16, 2023, SMITH's supervised release was revoked for the following violations: continued use of controlled substances, possession of drug paraphernalia, violation of the location monitoring program, unapproved contact with daughter, possession of pornography, and accessing the internet without approval. He was sentenced to five months in prison with no supervised release to follow. He was released from prison on September 22, 2023.

64. On November 7, 2024, SMITH registered with the State of Illinois as a sex offender. He reported an address of 1844 7th Street, Rock Island, Illinois. SMITH provided a phone number of (262) 344-0877 and email address of randycsmith1@gmail.com. SMITH is required to register as a sex offender until May 6, 2041.

TECHNICAL TERMS

65. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone

numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

d. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and

directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

e. Internet: The Internet is a global network of computers and other electronic device that communicate with each other. Due to the structure of the Internet, connections between device on the Internet often cross state and international borders, even when the device communicating with each other are in the same state.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook that is primarily operated by touching the screen. Tablets function as wireless communication device and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social network.

66. Based on my training, experience, and research, and from consulting the manufacturers' advertisements and product technical specifications available online at https://manuals.plus/vortex/a24-smart-phone-manual, https://www.samsung.com/us/smartphones/galaxy-a15/buy/galaxy-a15-5g-64gb-uscellular-sm-a156uzkbusc/, and https://www.samsung.com/us/business/support/owners/product/galaxy-a13-verizon/, I know that the Vortex, Model A24 cellular telephone cellular telephone, Samsung Galaxy A15, Model SM-A156U cellular telephone, and Samsung Galaxy A13, Model SM-A135U cellular telephone have capabilities that allow them to serve all or

some of the following functions: wireless telephone, a digital camera, GPS navigation device, and accessing /downloading information from the Internet. In my training and experience, examining data stored on devices of these types can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

67. Based on my knowledge, training, and experience, I know that an electronic device can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

68. As explained below, information stored within a cellular phone or tablet may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored within the device can indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, contacts lists, instant messaging logs, and communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the device at a relevant time. Further, such stored electronic data can show how and when the device and its related account were accessed or used. Such "timeline" information allows investigators to understand the chronological context of

device access, use, and events relating to the crime under investigation. This "timeline" information may tend to either inculpate or exculpate the device account owner. Additionally, information stored within a device may indicate the geographic location of the device and user at a particular time (e.g., location integrated into an image or video sent via email or text message to include both metadata and the physical location displayed in an image or video). Last, stored electronic data may provide relevant insight into the device owner's state of mind as it relates to the offense under investigation. For example, information in the device may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement). Unless this data is destroyed, by breaking the device itself or by a program that deletes or over-writes the data contained within the device, such data will remain stored within the device indefinitely.

69. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a

deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to obtain unauthorized access to a victim electronic device over the Internet the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

70. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

71. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

72. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

ATTACHMENT A

The property to be searched are as follows:

a. black Vortex, Model A24 cellular telephone, barcode: 3020240921170144412923, IMEI #: 358645341772515.

b. black Samsung Galaxy A15, Model SM-A156U cellular telephone, IMEI #: 358103210458931.

c. black Samsung Galaxy A13, Model SM-A135U cellular telephone, IMEI #: 357630390330382.

The Devices are currently located at the U.S. Department of Homeland Security-Homeland Security Investigations evidence locker located at 790 North Milwaukee Street, #600, Milwaukee, Wisconsin 53202.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of 18 USC 2252 and 2252A, including:

   a. Records containing child pornography or pertaining to the production, distribution, receipt, or possession of child pornography;

   b. Records or information, photographs, videos, notes, documents, or correspondence, in any format or medium, concerning communications about child pornography or sexual activity with or sexual interest in minors.

2. All names, aliases, and numbers stored in the Devices, including numbers associated with the Devices, relating to the identities of those engaged in the production, possession, receipt, or distribution of child pornography.

3. Images or visual depictions of child pornography.

4. Records and information containing child erotica, including texts, images, and visual depictions of child erotica.

5. Any and all information, notes, software, documents, records, or correspondence, in any format and medium, pertaining to the violations.

6. Any and all address books, names, and lists of names and addresses of individuals who may have been contacted by use of the computer or by other means for the purpose of committing the violations.

7. The list of all telephone calls made or received located in the memory of the Devices that provides information regarding the identities of and the methods and means of operation and communication by those engaged in the possession, receipt, or distribution of child pornography.

8. Any and all information, notes, documents, records, or correspondence, in any format or medium, concerning membership in online groups, clubs, or services that provide or make accessible child pornography.

9. Any and all information, records, documents, invoices, and materials, in any format or medium, that concern e-mail accounts, online storage, or other remote computer storage pertaining to the violations.

10. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.